Order Code RL31787

Information Operations and Cyberwar: Capabilities and Related Policy Issues

Updated September 14, 2006

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
14 SEP 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Operations and Cyberwar: Capabilities and Related Policy Issues	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service The Library of Congress 101 Independence Ave SE Washington, DC 20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**17**	

Information Operations and Cyberwar: Capabilities and Related Policy Issues

Summary

This report describes the emerging areas of information operations in the context of U.S. national security. It assesses known U.S. capabilities and plans, and suggests related policy issues of potential interest to Congress. This report will be updated to accommodate significant changes.

For military planners, the control of information is critical to military success, and communications networks and computers are of vital operational importance. The use of technology to both control and disrupt the flow of information has been referred to by several names: information warfare, electronic warfare, cyberwar, netwar, and Information Operations (IO). The U.S. Department of Defense has grouped IO activities into five core capabilities: Psychological Operations, Military Deception, Operational Security, Computer Network Operations, and Electronic Warfare.

Doctrine for U.S. IO now places new emphasis on Psychological Operations to influence the decisionmaking of possible adversaries, and on Electronic Warfare to dominate the entire electromagnetic spectrum. Some weapons used for IO are also referred to as "non-kinetic," and include high power microwave (HPM) or other directed electromagnetic energy weapons that rely on short powerful electromagnetic pulses (EMP), that can overpower and permanently degrade computer circuitry.

Several public policy issues that Congress may choose to consider include whether the United States should:

- encourage or discourage international arms control for cyberweapons, as other nations increase their cyber capabilities;
- modify U.S. cyber-crime legislation to conform to international agreements that make it easier to track and find cyber attackers;
- engage in covert psychological operations potentially affecting domestic audiences; or,
- create new regulation to hasten improvements to computer security for the nation's privately-owned critical infrastructure.

Contents

Information Operations and Cyberwar: Capabilities and Related Policy Issues

Introduction

Background

Control of information has always been part of military operations. However, the U.S. Strategic Command (USSTRATCOM) reportedly now views information operations as a core military competency, with new emphasis on (1) use of electromagnetic energy or cyberattack to control or disable an adversary's computers, and (2) use of psychological operations to manipulate an adversary's perceptions.[1]

The Department of Defense (DOD) view is that information itself is now a realm, a weapon, and a target of warfare. With current digital technology, the U.S. military now has the capability to act directly upon and alter the stored bits of computer code that comprise information inside the computers or on the networks of adversaries. In addition, DOD asserts that Psychological Operations, including the ability to rapidly disseminate persuasive information to diverse audiences in order to directly influence their decisionmaking, is an increasingly powerful means of deterring aggression, and an important method for undermining the leadership and popular support for terrorist organizations.[2]

However, new technologies for military information operations also create new national security vulnerabilities and new policy issues, including (1) possible international arms control policy for cyberweapons; (2) a need for international cooperation for pursuit of cyber terrorists and other cyber attackers; (3) consideration of psychological operations used to affect friendly nations; (4) a need to raise the computer security awareness of the civilian community; and (5) possible accusations of war crimes if offensive military cyberweapons severely disrupt critical civilian computer systems, or the systems of other non-combatant nations.

This report describes Department of Defense capabilities for conducting military information operations, and gives an overview of related policy issues.

---

[1] Jason Ma, "Information Operations To Play a Major Role in Deterrence Posture,"*Inside Missile Defense,* Dec. 10, 2003 [http://www.insidedefense.com/secure/defense_docnum.asp?f=defense_2002.ask&docnum=MISSILE-9-25-4].

[2] DOD Information Operations Roadmap, October 30, 2004, p.3. This document was declassified January, 2006, and obtained through FOIA by the National Security Archive at George Washington University. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

Definitions

Information

Information is a resource created from two things: phenomena (data) that are observed, plus the instructions (systems) required to analyze and interpret the data to give it meaning. The value of information is enhanced by technology, such as networks and computer databases, which enables the military to (1) create a higher level of shared awareness, (2) better synchronize command, control, and intelligence, and (3) translate information superiority into combat power.

DOD Information Operations

The DOD term for military information warfare is Information Operations (IO). DOD information operations are actions taken during time of crisis or conflict to affect adversary information, while defending one's own information systems, to achieve or promote specific objectives.[3] The focus of IO is on disrupting or influencing an adversary's decision-making processes.

An IO attack may take many forms, for example: (1) to slow adversary computers, the software may be disrupted by transmitting a virus or other cyberweapon (see section on cyberweapons below); (2) to disable sophisticated adversary weapons, the computer circuitry may be overheated with directed high energy pulses; and (3) to misdirect enemy radar, powerful signals may be broadcast to create false images. Other methods for IO attack may include initiating TV and radio broadcasts to influence the opinions and actions of a target audience, or seizing control of network communications to disrupt an adversary's unity of command.

Computer Network Defense (CND) is the term used to describe IO procedures that are designed to protect U.S. forces against IO attack from adversaries. Information Assurance (IA), which is part of CND, requires close attention to procedures for computer and information security (see Computer Network Operations below).

DOD states that IO must become a core military competency on a par with air, ground, maritime, and special operations. Accordingly, new emphasis is now placed on the importance of dominating the entire electromagnetic spectrum with new attack capabilities, including methods for computer network attack and electronic warfare. DOD also emphasizes that because networks are increasingly the operational center of gravity for warfighting, the U.S. military must be prepared to "fight the net".[4] Because the recently declassified source document containing this phrase has some lines blacked out, it is not clear if "...net" includes the Internet. If so, then this phrase may be a recognition by DOD that Psychological Operations, including public affairs

---

[3] From the *DOD Dictionary of Military and Associated Terms*, Jan. 2003 [http://www.dtic.mil/doctrine/jel/doddict/data/i/index.html].

[4] DOD Information Operations Roadmap, October 30, 2003, p.6-7. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

work and public diplomacy, must be employed in new ways to counter the skillful use of the Internet and the global news media by adversaries.

DOD Information Operations Core Capabilities

DOD identifies five core capabilities for conduct of information operations: (1) Psychological Operations, (2) Military Deception, (3) Operations Security, (4) Computer Network Operations, and (5) Electronic Warfare. These capabilities are interdependent, and increasingly need to be integrated to achieve desired effects, such as undermining the adversary's confidence in his own capabilities.

Psychological Operations (PSYOP)

DOD defines PSYOP as planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.[5] For example, during Operation Iraqi Freedom (OIF), broadcast messages were sent from Air Force EC-130E aircraft, and from Navy ships operating in the Persian Gulf, along with a barrage of e-mail, faxes, and cell phone calls to numerous Iraqi leaders encouraging them to abandon support for Saddam Hussein.

At the same time, the civilian Al Jazeera news network, based in Qatar, beams its messages to well over 35 million viewers in the Middle East, and is considered by many to be a "market competitor" for U.S. PSYOP. Terrorist groups can also use the Internet to quickly place their own messages before an international audience. Some observers have stated that the U.S. will continue to lose ground in the global media wars until it develops a coordinated strategic communications strategy to counter competitive civilian news media, such as Al Jazeera.[6]

Partly in response to this observation, DOD now emphasizes that PSYOP must be improved and focused against potential adversary decisionmaking, sometimes well in advance of times of conflict. Products created for PSYOP must be based on in-depth knowledge of the audience's decision-making processes. Using this knowledge, the PSYOP products then must be produced rapidly, and disseminated directly to targeted audiences throughout the area of operations.[7]

DOD policy restricts the use of PSYOP for targeting American audiences. However, while military PSYOP products are intended for foreign targeted audiences, DOD also acknowledges that the global media may pick up some of these

---

[5] *DOD Dictionary of Military Terms* [http://www.dtic.mil/doctrine/jel/doddict/].

[6] Air Force, *Operation Iraqi Freedom Information Operations Lessons Learned: First Look*, AFC2ISRC/CX, July 23, 2003 [http://www.insidedefense.com/secure/data_extra/pdf3/dplus2004_265.pdf].

[7] DOD Information Operations Roadmap, October 30, 2003, p.6. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

targeted messages, and replay them back to the U.S. domestic audience. Therefore, the distinction between foreign and domestic audiences cannot be maintained.[8]

Military Deception (MILDEC)

Deception guides an enemy into making mistakes by presenting false information, images, or statements. MILDEC is defined as actions executed to deliberately mislead adversary military decision makers with regard to friendly military capabilities, thereby causing the adversary to take specific actions (or fail to take) that will contribute to the success of the friendly military operation.

As an example of deception during OIF, the U.S. Navy deployed the Tactical Air Launched Decoy system to divert fire from Iraqi air defenses away from other real combat aircraft.

Operational Security (OPSEC)

OPSEC is defined as a process of identifying information that is critical to friendly operations and which could enable adversaries to attack operational vulnerabilities. For example, during OIF, U.S. forces were warned to remove certain information from DOD public websites, so that Iraqi forces could not exploit sensitive but unclassified information.

Computer Network Operations (CNO)

CNO includes the capability to: (1) attack and disrupt enemy computer networks; (2) defend our own military information systems; and (3) exploit enemy computer networks through intelligence collection.[9] Reportedly, a new U.S. military organization, called the Joint Functional Component Command for Network Warfare (JFCCNW), is responsible for the evolving mission of Computer Network Attack. The capabilities of the JFCCNW are highly classified, and DOD officials have reportedly never admitted to launching a cyber attack against an enemy, however many computer security officials believe the organization can destroy networks and penetrate enemy computers to steal or manipulate data, and take down enemy command-and-control systems. They also believe that the organization consists of personnel from the CIA, National Security Agency, FBI, the four military branches, and civilians and military representatives from allied nations.[10]

Computer Network Defense (CND). CND is defined as defensive measures to protect information, computers, and networks from disruption or destruction. CND includes actions taken to monitor, detect, and respond to unauthorized computer activity. Responses to IO attack against U.S. forces may

---

[8] DOD Information Operations Roadmap, October 30, 2003, p.26. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

[9] US Strategic Command Fact File [http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm].

[10] John Lasker, *U.S. Military's Elite Hacker Crew*, April 18, 2005, Wired News, [http://www.wired.com/news/privacy/0,67223-0.html?tw=wn_story_page_prev2].

include use of passive information assurance tools, such as firewalls or data encryption, or may include actions such as monitoring adversary computers to determine their capabilities before they attempt an IO attack against U.S. forces.

DOD believes that CND may lack sufficient policy and legal analysis for guiding appropriate responses to intrusions or attacks on DOD networks. Therefore, DOD has recommended that a legal review be conducted to determine what level of data manipulation constitutes an attack. The distinction is necessary in order to clarify whether an action should be called an attack or an intelligence collection operation, and which aggressive actions can be appropriately taken in self-defense. This legal review should also determine if appropriate authorities permit U.S. forces to retaliate through unwitting computer hosts. And finally, DOD has recommended structuring a legal regime that applies separately to domestic and to foreign sources of CNA against DOD or the U.S. infrastructure.[11]

Computer Network Exploitation (CNE). CNE is an area of Information Operations that is not yet clearly defined within DOD. Before a crisis develops, DOD seeks to prepare the IO battlespace through intelligence, surveillance, and reconnaissance, and through extensive planning activities. This involves espionage, that in the case of IO, is usually performed through network tools that penetrate adversary systems to return information about system vulnerabilities, or that make unauthorized copies of important files. Tools used for CNE are similar to those used for CNA, but configured for intelligence collection rather than system disruption.

Computer Network Attack (CNA). CNA is defined as operations to disrupt or destroy information resident in computers and computer networks. As a distinguishing feature, CNA relies on a data stream used as a weapon to execute an attack. For example, sending a digital signal stream through a network to instruct a controller to shut off the power flow is CNA, while sending a high voltage surge through the electrical power cable to short out the power supply is Electronic Warfare.

During Operation Iraqi Freedom, U.S. and coalition forces reportedly did not carry out computer network attacks against Iraqi systems. Even though comprehensive IO plans were prepared in advance, several DOD officials reportedly stated that top-level approval for several computer attack missions was not granted until it was too late to carry them out to achieve war objectives.[12] U.S. officials reportedly may have rejected launching a planned cyber attack against Iraqi financial computers because Iraq's banking network is connected to a financial communications network located in Europe. According to Pentagon sources, an IO attack directed at Iraq might also have brought down banks and ATM machines located in parts of Europe as well. Such global network interconnections, plus close network links between Iraqi military computer systems and the civilian infrastructure,

---

[11] DOD Information Operations Roadmap, October 30, 2003, p52. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

[12] Elaine Grossman, "Officials: Space, Info Targets Largely Cobbled On-The-Fly for Iraq," *Inside the Pentagon*, May 29, 2003.

reportedly frustrated attempts by U.S. forces to design a cyber attack that would be limited to military targets only in Iraq.[13]

Cyberweapons. Cyberweapons are computer programs capable of disrupting the data storage or processing logic of enemy computers. Cyberweapons include (1) offensive attack tools, such as viruses, Trojan horses, denial-of-service attack tools; (2) "dual use" tools, such as port vulnerability scanners, and network monitoring tools; and, (3) defensive tools, such as encryption and firewalls.

Cyberweapons are becoming easier to obtain, easier to use, and more powerful. In a 1999 study, the National Institute of Standards and Technology (NIST) found that many newer attack tools, available on the Internet, can now easily penetrate most networks, and many others are effective in penetrating firewalls and attacking Internet routers. Other tools allow attacks to be launched by simply typing the Internet address of a designated target directly into the attack-enabling website.[14]

In a meeting held in January 2003, at the Massachusetts Institute of Technology, White House officials sought input from experts outside government on guidelines for use of cyberweapons. Officials have stated they are proceeding cautiously, since a cyberattack could have serious cascading effects, perhaps causing major disruption to networked civilian systems.[15]

In February 2003, the Bush Administration announced developed national-level guidance for determining when and how the United States would launch computer network attacks against foreign adversary computer systems. The classified guidance, known as National Security Presidential Directive 16 (classified), is intended to clarify circumstances under which an attack would be justified, and who has authority to launch a computer attack.

Electronic Warfare (EW)

EW is defined as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. High power electromagnetic energy can be used as a tool to overload or disrupt the circuitry of electronic equipment, such as computers, radios, telephones, and almost anything that uses transistors, circuits, and wiring.[16]

Domination of the Electromagnetic Spectrum. Electronic Warfare tools include weapons for jamming or overpowering enemy communications and

---

[13] Charles Smith, "U.S. Information Warriors Wrestle with New Weapons," *NewsMax.com*, March 13, 2003 [http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml].

[14] Dorothy Denning, "Reflections on Cyberweapons Controls," *Computer Security Journal*, XVI, 4, Fall, 2000, p.43-53.

[15] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washington Post*, February 7, 2003, Section A, p.1.

[16] CRS Report RL32544, *High Altitude Electromagnetic Pulse (EMP) and High Power Microwave (HPM) Devices: Threat Assessments*, by Clay Wilson.

telemetry, and weapons that overheat circuitry. DOD now emphasizes maximum control of the entire electromagnetic spectrum, including disrupting the full spectrum of emerging communication systems, sensors, and weapons systems. This may include (1) navigation warfare, including offensive space operations where global positioning satellites may be disrupted; or, (2) methods to control adversary radio systems that help them identify friend and foe; and, (3) methods to disrupt radar systems, directed energy weapons, unmanned aerial vehicles (UAVs), or robots operated by adversaries.[17]

Recent military IO testing examined the capability to secretly enter an enemy computer network and monitor what their radar systems could detect. Further experiments tested the capability to take over enemy computers and manipulate their radar to show false images.[18]

Non-Kinetic Weapons. "Non-kinetic" is a term that is sometimes used to describe non-explosive weapons with capabilities for disabling enemy computer systems. These weapons emit directed electromagnetic energy that, in short pulses, may disable computer circuitry, or in other applications. For example, a non-kinetic weapon might disable an approaching enemy missile by directing a High Power Microwave (HPM) beam that burns out the circuitry, or by sending a false telemetry signal that misdirects the targeting computer.[19]

During OIF, many Iraqi command bunkers were deeply buried underground and proved difficult to attack using conventional explosives. However, new HPM weapons were reportedly considered for possible use in attacks against these targets because the numerous communications and power lines leading into the underground bunkers offered pathways for conducting powerful surges of electromagnetic energy that could destroy the computer equipment inside.[20]

Current DOD Command Structure for Information Operations

The U.S. Strategic Command (USSTRATCOM), a unified combatant command for U.S. strategic forces, controls military space operations, information operations, strategic warning and intelligence assessments, global strategic operations planning,

---

[17] DOD Information Operations Roadmap, October 30, 2003, p.61. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

[18] These programs were called Suter 1 and Suter 2, and were tested during Joint Expeditionary Forces Experiments held at Nellis Air Force Base in 2000 and 2002. David Fulghum, "Sneak Attack," *Aviation Week & Space Technology*, June 28, 2004, p. 34.

[19] David Fulghum, "Sneak Attack," *Aviation Week & Space Technology*, June 28, 2004, p.34.

[20] Will Dunham, "U.S. May Debut Secret Microwave Weapon versus Iraq," *Reuters*, February 2, 2003 [http://www.globalsecurity.org/org/news/2003/030202-ebomb01.htm].

and also has overall responsibility for Computer Network Operations (CNO).[21] Much information about CNO, which includes defense against cyber attack and security breaches, as well as the related area of offensive computer network attack, is classified.

The USSTRATCOM exercises command authority over several Joint Functional Component Commands (JFCCs): (1) space and global strike; (2) intelligence, surveillance and reconnaissance; (3) network warfare; integrated missile defense; and (4) combating weapons of mass destruction.[22] The JFCCs with responsibility for DOD cyber security are the JFCC-Network Warfare (JFCC-NW), and the JFCC-Space & Global Strike (JFCC-SGS) which also houses the Joint information Operations Warfare Center (JIOWC). A third organization called the Joint Task Force-Global Network Operations (JTF-GNO), also has responsibility for DOD cyber security. The DOD organizations with major responsibility for defense against cyber attack are the JIOWC and the JTF-GNO.[23]

The JTF-GNO is the organization responsible for operating and defending the DOD information infrastructure (the infrastructure is called the Global Information Grid). The JFCC-NW is responsible for deliberate planning of network warfare, which includes coordinated planning of offensive network attack. The JIOWC is responsible for assisting combatant commands with an integrated approach to information operations. These include operations security, psychological operations, military deception, and electronic warfare. It coordinates network operations and network warfare with the JTF-GNO and with JFCC-NW.

Policy Issues

Potential oversight issues for Congress may include the following:

- Effects of international arms control for cyberweapons;
- Need for international cooperation for pursuit of cyber terrorists and other cyber attackers;
- Use of psychological operations that may affect domestic audiences, and;

---

[21] United States Strategic Command, July 2006, [http://www.stratcom.mil/organization-fnc_comp.html].

[22] United States Strategic Command, July 2006, [http://www.stratcom.mil/organization-fnc_comp.html].

[23] Clark A. Murdock et. al, *Beyond Goldwater-Nichols: U.S. Government and Defense Reform for a New Strategic Era, Phase 2 Report*, July 2005,Center for Strategic and International Studies, p.128, [http://www.ndu.edu/library/docs/BeyondGoldwaterNicholsPhase2Report.pdf].

- Need to raise the computer security awareness of the U.S. private sector and civilian population to better protect national security.

International Arms Control for Cyberweapons

Should the United States adopt a position to encourage or discourage international controls for weapons in cyberspace, especially as other nations, such as Iran, China, and Russia increase their cyber capabilities? Attacks against information systems using computer viruses could be considered an act of war within the scope of the laws of armed conflict, and some international organizations are now attempting to classify and control malicious computer code In 1998 and 1999, Russia proposed that the First Committee of the United Nations explore an international agreement on the need for arms controls for information warfare weapons. The G-8 Government-Industry Conference on High Tech Crime in 2002 also sought international agreement on ways to classify and control malicious computer code. [24]

DOD has not yet developed a policy regarding international controls for cyberweapons, however, the United States remains concerned about future capabilities for foreign nations to develop their own effective capabilities for computer espionage and computer network attack.[25] For example, the Chinese military is enhancing its information operations capabilities, according to the Defense Department's annual report to Congress on China's military prowess.[26] The report finds that China is placing specific emphasis on the ability to perform information operations designed to weaken an enemy force's command and control systems.[27]

Council of Europe Convention on Cybercrime

Military officials have reportedly stated that other nations, rather than terrorist groups, pose the biggest threat to U.S. computer networks.[28] However, the intent of a cyberattack directed against U.S. computer systems, as well as the identity of the

---

[24] The G-8 included France, Germany, Japan, United Kingdom., United States, Italy, Canada, and Russia. Denning, "Reflections on Cyberweapons Controls," *Computer Security Journal*, XVI, 4, Fall, 2000, p. 43-53. Andrew Rathmell, "Controlling Computer and Network Operations," *Information and Security*, vol. 7, 2001, pp. 121-144.

[25] A US Air Force-sponsored workshop held in March 2000 concluded that international efforts to tackle cybercrime and cyberterrorism "could hinder US information warfare capabilities, thus requiring new investments or new research and development to maintain capabilities." USAF Directorate for Nuclear and Counter proliferation and Chemical and Biological Arms Control Institute, *Cyberwarfare: What Role for Arms Control and International Negotiations?* (Washington, D.C., March 20, 2000).

[26] See the FY2004 Report to Congress on PRC Military Power, [http://www.defenselink.mil/pubs/d20040528PRC.pdf].

[27] John Bennett, "Commission: U.S. Should Push Beijing to up Pressure on North Korea," *Inside the Pentagon*, June 17, 2004.

[28] Mickey McCarter, "Computer Offensive," *Military Information Technology*, November 15, 2002 [http://www.mit-kmi.com/print_article.cfm?DocID=51] .

attacker, may be hard to determine. To pursue their IO objectives, some countries could rely on individual hackers who cannot be easily linked to a government. Also, what are the diplomatic and foreign policy implications that could result from the United States remotely, and with no advance notice, conducting computer surveillance that may intrude into the sovereignty of another nation?

An emerging issue is the degree to which the United States should pursue international agreements to harmonize cyber-crime legislation, and also deter cyber-crime through tougher criminal penalties. Pursuit to identify the source of a cyber attack often involves a trace back through networks that may require the cooperation of Internet service providers in different nations. The technical problems of pursuit and detection are more difficult if one or more of the nations involved has a legal policy that conflicts with that of the United States.[29]

The U.S. Senate voted on August 3, 2006 to ratify the Council of Europe Convention on Cybercrime.[30] The United States, acting as an observer at the Council of Europe, participated actively in the development of the Convention, which is the only multilateral treaty to address the problems of computer-related crime and electronic evidence gathering. The Administration has stated that the treaty will help deny a safe haven to criminals and terrorists who can cause damage to U.S. interests from abroad using computer systems.[31]

The treaty requires participating nations to update their laws to reflect computer crimes such as unauthorized intrusions into networks, the release of worms and viruses, and copyright infringement, however, the United States will comply with the Convention based on existing U.S. federal law; and no new implementing legislation will be required.[32] Among several reservations included in the U.S. Senate resolution

---

[29] In Argentina, a group calling themselves the X-Team, hacked into the website of the Supreme Court of Argentina in April 2002. The trial judge stated that the law in his country covers crime against people, things and animals but not websites. The group on trial was declared not guilty of breaking into the website. Paul Hillbeck, "Argentine Judge Rules in Favor of Computer Hackers," February 5, 2002 [http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3070194.htm].

[30] Carolee Walker, *U.S. Senate Votes To Ratify Cybercrime Convention*, USINFO, August 7, 2006, [http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2006&m=August&x=20060807133221bcreklaw0.5304834].

[31] Declan McCullagh, "Bush Pushes for Cybercrime Treaty," *CnetNews.com*, November 18, 2003, [http://news.com.com/2102-1028_3-5108854.html?tag=st.util.print]. U.S. Department of State, *Bush Asks Senate Approval to Ratify Convention on Cybercrime*, Bureau of International Information Programs, November 17, 2003, [http://usinfo.state.gov/xarchives/display.html?p=washfile-english&y=2003&m=November&x=20031117190405rennefl0.4209101&t=usinfo/wf-latest.html].

[32] Statement of Attorney General Alberto R. Gonzales on the Passage of the Cybercrime Convention, U.S. Department of Justice Press Release, August 4, 2006, [http://www.usdoj.gov/opa/pr/2006/August/06_ag_499.html]. See also, CRS Report RS21208, *Cybercrime: The Council of Europe Convention*, by Kristin Archick. Forty-six European Countries belong to the Council of Europe, which was founded in 1949. The United States, Japan, Canada, Mexico, and the Holy See (Vatican City) are granted observer status. The thirty eight Council of Europe member state signatories are Albania, Armenia,

of ratification, the United States reserves the right not to apply Article 6 of the treaty (this section discusses "Misuse of Devices") to devices that are designed for the purpose of committing offenses such as "Data interference" and "System interference".[33]

The treaty reportedly expands police search powers in some areas without corresponding privacy or due process protections, and requires police in participating nations to cooperate with police in other countries, including arrangements for mutual assistance and extradition among participating nations.[34] While some observers say that international cooperation is important for defending against cyber attacks and improving global cybersecurity, others point out that the treaty also contains a questionable Additional Protocol[35] that would require nations to imprison anyone guilty of "insulting publicly, through a computer system" certain groups of people based on characteristics such as race or ethnic origin. The U.S. delegation to the Council of Europe has reportedly argued that such an addition would violate of the First Amendment's guarantee of freedom of expression.[36] The Electronic Privacy Information Center has also objected to the additional protocol, saying that it would "would create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards."[37]

The Convention on Cybercrime became effective initially for the first five ratifying nations on July 1, 2004. The Additional Protocol, which has not been

---

Austria, Belgium, Bosnia-Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Serbia and Montenegro, Slovakia, Slovenia, Spain, Sweden, Switzerland, the Former Yugoslav Republic of Macedonia, Ukraine, and the United Kingdom. In addition to the United States, the convention has been ratified by 11other nations.

[33] Congressional Record, *Council of Europe Convention on Cybercrime*, Government Printing Office, August 3, 2006, p.S8901. Observers have stated that the discussion of "Illegal Devices" set out in Articles 6 of the convention may lack sufficient specificity to ensure that it will not become a basis to investigate individuals engaged in computer-related activity that is completely lawful, and may also discourage the development of new security tools and give government an improper role in policing scientific innovation. See Global Internet Liberty Campaign, October 18, 2000, [http://www.gilc.org/privacy/coe-letter-1000.html].

[34] Barry Steinhardt, *Three cheers for international cooperation*, Eurozine, October 25, 2005, [http://www.eurozine.com/articles/2005-10-25-steinhardt-en.html].

[35] Council of Europe, *Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*, November 2002, [http://www.cybercrime.gov/coehatespeechProtocol.pdf].

[36] Council of Europe, *Explanatory Report for the Additional Protocol to the Convention on Cybercrime*, paragraph 4, [http://conventions.coe.int/Treaty/en/Reports/Html/189.htm].

[37] Declan McCullagh, "Senate Debates Cybercrime Treaty," *CnetNews.com*, June 18, 2004, [http://news.com.com/2102-1028_3-5238865.html?tag=st.util.print] .

signed by the United States, became effective for the first five ratifying nations on March 1, 2006.[38]

Psychological Operations Affecting Domestic Audiences

Some observers have stated that success in future conflicts will depend less on the will of governments, and more on the perceptions of populations, and that perception control will be achieved and opinions shaped by the warring group that best exploits the global media.[39]

Executive Order 13283, signed by President George W. Bush on January 21, 2003, established within the White house the Office of Global Communications (OGC).[40] That office is currently studying ways to reach Muslim audiences directly through radio and TV, to counter anti-American sentiments.[41]

However, an emerging issue may be whether the Department of Defense is legislatively authorized to engage in PSYOP that may also affect domestic audiences.[42] DOD Joint Publication 3-13, released February 2006, provides current doctrine for U.S. military Information Operations. However, the DOD Information Operations Roadmap, published October 2003, states that PSYOP messages intended for foreign audiences increasingly are consumed by the U.S. domestic audience, usually because they can be rebroadcast through the global media. The DOD document states that, "...the distinction between foreign and domestic audiences becomes more a question of USG (U.S. Government) intent rather than information dissemination practices (by DOD)."[43] This may be interpreted to mean that DOD has no control over who consumes PSYOP messages once they are retransmitted by commercial media.

---

[38] As of December 2005, 29 members of the Council plus the United States, Canada, Japan, Montenegro, and South Africa have signed the additional Protocol, and eleven signatories have ratified it. See Council of Europe Convention on Cybercrime, December 2005, [http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=12/07/2005&CL=ENG], Council of Europe Additional Protocol the the Convention on Cybercrime, December 2005, [http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=12/07/2005&CL=EN].

[39] Maj. Gen. Robert Scales (Ret), *Clausewitz and World War IV*, Armed Forces Journal, July 2006, p.19.

[40] "Presidential Documents, Title 3 - The President - Establishing the Office of Global Communications," *Federal Register*, Vol. 68, no. 16, Jan. 24, 2003.

[41] OGC has been up and running since July 2002, working to get the Administration's message out to foreign news media outlets. Tucker Eskew stated that, "(The President) knows that we need to communicate our policies and values to the world with greater clarity and through dialogue with emerging voices around the globe." Scott Lindlaw, "New Office Aims to Bolster U.S. Image," *AP Online*, Feb. 11, 2003.

[42] Psychological Operations are authorized for the military under Title 10, USC, Subtitle A, Part I, Chapter 6, Section 167.

[43] DOD Information Operations Roadmap, October 30, 2003, p.26. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf]

In addition, observers have stated that terrorists, through use of the Internet, are now challenging the monopoly over mass communications that both state-owned and commercial media have long exercised. A strategy of the terrorists is to propagate their messages quickly and repeat them until they have saturated cyberspace. Internet messages by terrorist groups have become increasingly sophisticated through use of a cadre of Internet specialists who operate computer servers worldwide. Other observers have also stated that al-Qaeda now relies on a Global Islamic Media Unit to assist with its public outreach efforts.[44]

As a result of the increasingly sophisticated use of networks by terrorist groups and the potentially strong influence of messages carried by the global media, does DOD now view the Internet and the mainstream media as posing a vital threat to its mission? Will PSYOP be used to manipulate public opinion, including domestic audiences, to reduce opposition to unpopular decisions in the future?

Role of the U.S. Private Sector in Protecting Computer Security

The National Strategy to Secure Cyberspace,[45] published February 2003, states that the private sector now has a crucial role in protecting national security because it largely runs the nation's critical infrastructure.[46] Richard Clarke, former chairman of the Critical Infrastructure Protection Board (CIPB), has also stated that the United States critical infrastructure is particularly vulnerable to IO attack because cyber attackers could possibly use the millions of home and business PCs, that are poorly protected against malicious code, to launch and support a series of debilitating assaults. The National Strategy urges home and small business computer users to install firewalls and antivirus software, and calls for a public-private dialogue to devise ways that the government can reduce the burden of security on home users and businesses.

To help raise awareness about national security vulnerabilities to possible cyber attack by hackers, or IO attack by adversaries, DOD has prepared a series of DVD and web-based training products that provide information about internal and external threats to information systems. Several are designed specifically for users of federal computer systems, and some are intended for users who are not information

---

[44] Jacquelyn S. Porth, *Terrorists Use Cyberspace as Important Communications Tool*, U.S. Department of State, USInfo.State.Gov, May 5, 2006, [http://usinfo.state.gov/is/Archive/2006/May/08-429418.html].

[45] See the full text for National Strategy to Secure Cyberspace at [http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf].

[46] The plan identifies 24 strategic goals and gives more than 70 recommendations on how various communities can secure their part of cyberspace. The communities are broken down into five levels (the home user, the large enterprise, critical sectors, the nation, and the global community). [http://www.whitehouse.gov/pcipb/]

technology professionals, but who need to understand the DOD and civilian communications infrastructure.[47]

However, some observers in the private sector feel the plan described in the National Strategy to Secure Cyberspace does not do enough to ensure that companies will adopt sound security practices, and suggest regulation is needed to supplement, or replace market forces.[48] For example, the congressionally appointed Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, chaired by former Virginia Governor James S. Gilmore III, has strongly criticized a draft of the plan. In its fourth volume, the Gilmore Report indicates that public/private partnerships and market forces are not working to protect national security in cyberspace. The Gilmore Report faults the National Strategy Plan for relying too heavily on persuasion to get the private sector to act, and for not holding managers accountable for improving cybersecurity for the systems they own and operate.[49]

Should the National Strategy to Secure Cyberspace contain language that compels the private sector to adopt stronger cybersecurity measures to protect national security in cyberspace?

Current Legislation

H.R. 1869, the Strategic Communication Act of 2005, was introduced in the House on April 27, 2005, and was referred on the same day to the Committee on International Relations. The bill is intended to improve the conduct of strategic communication by the Federal Government. Section 3 of the Bill requires the Secretary of State to report to Congress a description of efforts taken to coordinate the components of strategic communication, including components related to public diplomacy, public affairs, international broadcasting, and military information operations.

---

[47] DOD Information Assurance Training and Awareness Products, [http://www.securitymanagement.com/library/training_tech0902.pdf].

[48] Brian Krebs, "White House Releases Cybersecurity Plan," *Washingtonpost.com*, February 14, 2003.

[49] *Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* , p.81, [http://www.rand.org/nsrd/terrpanel/terror4.pdf].